



Reply to Attn of:

Office of the Chief Information Officer

MAY 21 2009

TO: Distribution

FROM: Deputy Chief Information Officer for IT Security

SUBJECT: Certification and Accreditation Notices

This document provides guidance in the form of four notices regarding NASA's certification and accreditation activities.

The first notice reminds system owners of their responsibilities to certify and accredit Federal information systems. The second notice articulates NASA's decision regarding the use of internal independent certifiers to certify security controls for FY09 and FY10. The third notice rescinds, in part, the September 17, 2008 decision to utilize the Bureau of Public Debt (BPD) to conduct security certifications. The fourth notice rescinds, in part, the November 29, 2007 decision to require annual recertification of common controls.

Responsibility to Certify and Accredit Federal Information Systems

The Office of Management and Budget (OMB) Circular number A-130, *Management of Federal Information Resources*, establishes the policy for management of Federal information resources.

Appendix III¹, *Security of Federal Automated Information Resources*, establishes a minimal set of security controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123.

One of the minimal controls established in A-130 includes:

"Authorize Processing. Ensure that a management official authorizes in writing use of the application by confirming that its security plan as implemented adequately secures the application. Results of the most recent review or audit of controls shall be a factor in management authorizations. The application must be authorized prior to operating and re-authorized at least every three years thereafter. Management authorization implies accepting the risk of each system used by the application"

¹ http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

Authorized processing and the recent review or audit of controls is synonymous with certification and accreditation (C&A).

Furthermore, the Federal Information Security Management Act (FISMA), Subchapter III, Information Security², among many requirements,

“provide[s] for development and maintenance of minimum controls required to protect Federal information and information systems”

In 2007, NASA certified and accredited 96% of its systems. Certifying and accrediting systems is a three year activity. If there is a significant change to the system that result in a significant change to the security posture, then the system must be recertified and reaccredited to continue operating.

Fiscal year 2010 will mark the expiration of Authorization to Operate (ATO) for many systems that were certified and accredited during the 2007 C&A activity.

It is imperative that NASA system owners recertify and reaccredit their information systems prior to the expiration of the current ATO date. Compliance with OMB A-130 and FISMA is mandatory.

Since 2007, the NASA Office of the Chief Information Officer (OCIO) has maintained a contract vehicle whereby security certification services can be purchased by system owners. The certification services are provided by a third-party that is independent with respect to the developmental, operational, and/or management chain of command associated with the information system³.

Systems owners, who have not begun to recertify and reaccredit systems under their purview, are strongly encouraged to schedule the security certification activity immediately. Contact information for scheduling third-party independent certification activities is provided on the last page of this memorandum.

Security Control Assessor (Independent Certifier) Decision

The draft versions of NIST Special Publication 800-37 revision 1, *Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach*, and NIST Special Publication 800-53 revision 3, *Recommended Security Controls for Federal Information Systems*, allow for flexibility in the selection of a security control assessor with the application of specific criteria for determining *independence*. While this flexibility is certainly desirable, the guidance is still in draft form and NASA has not had the opportunity to weigh in on the specific criteria needed to determine such independence. Additionally, the NASA Office of the Chief Information Officer (OCIO) does not believe that there is a sufficient level of knowledge, skill and ability, or resources currently within NASA to perform internal and independent assessments with a great deal of consistency for all systems.

² <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>

³ <http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf>

Even in the event that the NIST publications were made final in the very near future, there would not be sufficient time to stand-up an enterprise-wide education and training capability, identify the appropriate personnel, create and implement new policy and guidance and execute an independent assessor capability prior to the September 2010 recertification deadline.

To this end, the agency, at this time, will not support, approve or deem credible an independent certification activity using NASA staff for systems that are categorized as moderate or high. Any moderate or high system that is reported as completing certification and accreditation using NASA staff as independent certifiers will not be reflected in the FISMA report or the Exhibit 300 submitted to OMB and Congress as having been certified and accredited.

Rescinding Requirement to Utilize Bureau of Public Debt

The OCIO is formally rescinding the requirement, as originally stated in my September 17, 2008 memorandum, to enter into a contractual agreement with the Bureau of Public Debt (BPD) to provide third-party independent security certification services. The reason for this decision is based on the information that OCIO received on April 15, 2009 from the Information Systems Security Line of Business Program Management Office (ISS LoB PMO) at the Department of Homeland Security (DHS). At that time, the ISS LoB PMO stated that although several Federal agencies had been selected as Shared Service Centers (SSC) to provide security certification services, agencies were not required to utilize those services and could continue using services already in effect at their respective agencies. The decision to transition to a designated SSC was left to the discretion of the agency. OCIO believes that it is in the best interest of the C&A program to continue with its current service provider to avoid program disruption.

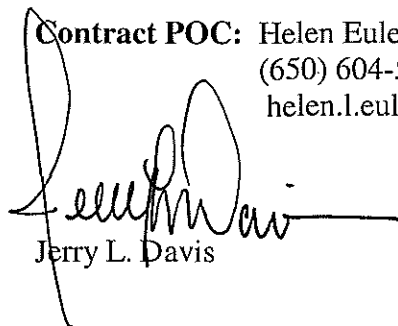
Rescinding Requirement to Annually Certify Common Controls

The OCIO is formally rescinding the requirement, as originally stated in my November 29, 2007 memorandum, to certify all common controls annually. Continuous monitoring, as indicated in NASA Information Technology Requirement (NITR) 2810-12, *Continuous Monitoring*, will provide the necessary oversight and requirement to assess common controls annually.

Contact information for scheduling third-party independent certification activities is provided below:

NASA's Independent Certifier: SecureInfo

Contract POC: Helen Euler, Project Manager
(650) 604-5541
helen.l.euler@nasa.gov



Jerry L. Davis

DISTRIBUTION:

Center CIOs:

ARC/Christopher Kemp

DFRC/Robert Binkley

GRC/Dr. Sasi Pillay

GSFC/Linda Cureton

HQ/Victor Thompson (Acting)

JPL/Jim Rinaldi

JSC/Larry Sweet

KSC/Mike Bolger

LaRC/Cathy Mangum

MSFC/Jonathan Pettus

NSSC/James Cluff

SSC/Gay Irby